

**PCT**  
 WELTORGANISATION FÜR GEISTIGES EIGENTUM  
 Internationales Büro  
 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
 INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

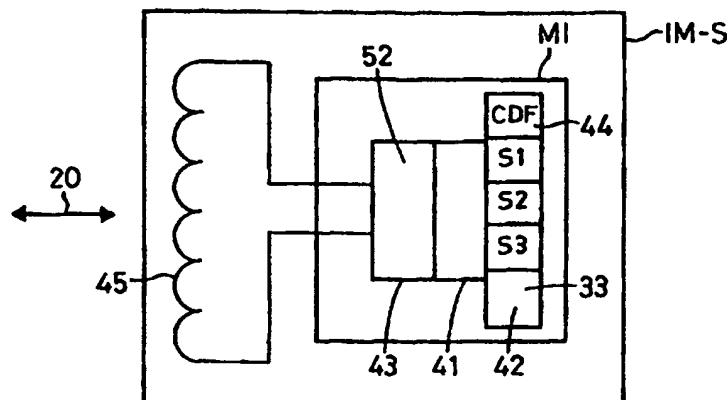


<b>(51) Internationale Patentklassifikation <sup>6</sup> :</b> <b>G07F 7/10</b>	<b>A1</b>	<b>(11) Internationale Veröffentlichungsnummer:</b> <b>WO 97/34265</b>  <b>(43) Internationales Veröffentlichungsdatum:</b> 18. September 1997 (18.09.97)
------------------------------------------------------------------------------------	-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

<p><b>(21) Internationales Aktenzeichen:</b> PCT/CH97/00063</p> <p><b>(22) Internationales Anmeldedatum:</b> 19. Februar 1997 (19.02.97)</p> <p><b>(30) Prioritätsdaten:</b>          628/96                      11. März 1996 (11.03.96)                      CH</p> <p><b>(71) Anmelder (für alle Bestimmungsstaaten ausser US):</b> KABA SCHLIESSTSYSTEME AG [CH/CH]; Mühlebühlstrasse 23, CH-8620 Wetzikon (CH).</p> <p><b>(72) Erfinder; und</b>  <b>(75) Erfinder/Anmelder (nur für US):</b> LOCHER, Johann [CH/CH]; Ettenhauserstrasse 67, CH-8620 Wetzikon (CH). GRAF, Ulrich [CH/CH]; Arbergstrasse 53, CH-8405 Winterthur (CH).</p> <p><b>(74) Anwalt:</b> FREI PATENTANWALTSBÜRO; Hedwigsteig 6, Postfach 768, CH-8029 Zürich (CH).</p>	<p><b>(81) Bestimmungsstaaten:</b> AU, BR, CA, CN, JP, KR, MX, SG, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p><b>Veröffentlicht</b>  <i>Mit internationalem Recherchenbericht.</i></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**(54) Title:** IDENTIFICATION MEDIUM WITH PASSIVE ELECTRONIC DATA CARRIER

**(54) Bezeichnung:** IDENTIFIKATIONS-MEDIUM MIT PASSIVEM ELEKTRONISCHEM DATENTRÄGER



**(57) Abstract**

The invention relates to an identification medium with a passive electronic data carrier and non-contact, coded communication with an associated read and write station WR. Said medium has in a memory (42) data organisation with a common data field CDF, master data (44) which cannot be changed or copied, an application data field ADF which can be segmented and into which a plurality of independent applications can be input as application segments (S1, S2, S3). To this end, a hierarchical authorisation system A valid for all read and write stations WR is established, which system has to be used to initial each identification medium IM-S and ensures that none of the independent applications affect each other.

**(57) Zusammenfassung**

Das Identifikationsmedium mit passivem elektronischem Datenträger und berührungsloser codierter Kommunikation mit einer zugeordneten Schreib- und Lesestation WR weist in einem Speicher (42) eine Datenorganisation auf mit einem gemeinsamen Datenfeld CDF, mit unveränderbaren und nicht kopierbaren Stammdaten (44), mit einem segmentierbaren Applikationsdatenfeld ADF, in welchem mehrere unabhängige Applikationen in Applikationssegmente (S1, S2, S3) einschreibbar sind. Dabei ist ein für alle Identifikationsmedien IM-S und alle Schreib- und Lesestationen WR gültiges hierarchisches Autorisierungssystem A festgelegt, mit welchem jedes Identifikationsmedium IM-S initialisiert werden muss und welches die gegenseitige Unbeeinflussbarkeit aller unabhängigen Applikationen sicherstellt.

**LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

## IDENTIFIKATIONSMEDIUM MIT PASSIVEM ELEKTRONISCHEM DATENTRÄGER

Die Erfindung betrifft ein Identifikationsmedium mit passivem elektronischem Datenträger gemäss Oberbegriff von Patentanspruch 1, eine Anlage mit derartigen Identifikationsmedien nach Anspruch 17 und ein Verfahren zur Initialisierung eines Identifikationsmediums nach Anspruch 20. Derartige Identifikationsmedien sind für verschiedene Applikationen bekannt, z.B. als Zutrittskarten für bestimmte Bereiche einer Firma (elektronische Schlüssel), für die Zeitwirtschaft, als Zugangsmedien für die Benützung von Geräten, z.B. von Datenanlagen, oder auch als Wertkartensysteme zum Bezug von Leistungen. Für jede unabhängige Applikation ist dabei ein eigenes Medium z.B. in Form einer Karte oder eines elektronischen Schlüssels erforderlich. Eine neue Applikation, welche ein Benutzer anwenden will, erfordert wieder ein zusätzliches neues Medium. So muss ein Benutzer, der verschiedene Applikationen benutzen will, auch entsprechend viele einzelne Medien mitführen. Dies ist einerseits aufwendig und umständlich, und es besteht andererseits die Gefahr, eines dieser vielen Medien oder Karten zu verlieren oder zu vergessen und sie dann nicht zur Verfügung zu haben, wenn sie benötigt wird.

Es ist daher Aufgabe der vorliegenden Erfindung, diese Unzulänglichkeiten und Einschränkungen bisheriger Lösungen zu überwinden und ein Identifika-

- tionsmedium zu schaffen, mit welchem mehrere unabhängige Applikationen mit einem einzigem Medium benutzbar sind. Dabei sollte die Handhabung einfach, und berührungslos, aus Distanz (hands free) sicher funktionieren. Die Sicherheit der übertragenen Daten sollte dabei gewährleistet sein bezüglich
- 5 Störungen, Verlust wie auch bezüglich Betrugsversuchen, und die Unabhängigkeit der verschiedenen Applikationen muss so gesichert sein, dass keine unerwünschte Einflussnahme auf andere Applikationen möglich ist. Erwünscht ist auch, dass spätere zusätzliche Applikationen auch auf das selbe Identifikationsmedium aufgenommen werden können.
- 10 Diese Aufgabe wird erfindungsgemäss gelöst durch ein Identifikationsmedium gemäss Patentanspruch 1.
- Die abhängigen Patentansprüche betreffen vorteilhafte Weiterbildungen der Erfindung.
- Im folgenden wird die Erfindung anhand von Figuren und Beispielen weiter
- 15 erläutert. Es zeigen
- Fig. 1 ein erfindungsgemässes Identifikationsmedium mit segmentiertem Applikationsdatenfeld AD
- Fig. 2 eine zugeordnete dezentrale Schreib- und Lesestation WR
- 20 Fig. 3a, b den Aufbau eines Identifikationsmediums mit grossflächiger Antenne
- Fig. 4a, b Datenorganisationen mit gemeinsamem Datenfeld und segmentiertem Applikationsdatenfeld mit mehreren Applikationssegmenten
- 25 Fig. 5 eine Datenorganisation eines Applikationssegments mit Segment Header SCDF und Applikationsdatenfeld SADF
- Fig. 6 eine Datenorganisation eines Applikationssegments mit vererbtem Basisdatensatz (Stamp)
- Fig. 7 den Zusammenhang zwischen Organisationslevel und vererbtem
- 30 Basisdatensatz (Stamp)

- Fig. 8a, b das hierarchische Autorisierungskonzept A des Systems für alle Identifikationsmedien und alle zugeordneten Schreib- und Lesestationen mit Organisationslevels
- 5 Fig. 9 den Zusammenhang zwischen Organisationslevel und Datenorganisation
- Fig. 10 illustriert die nicht kopierbare Erzeugung von Identifikationsmedien
- Fig. 11 Funktion und Ablauf der Kommunikation zwischen einem Identifikationsmedium und einer Schreib- und Lesestation
- 10 Fig. 12 die Funktion eines Schattenspeichers im Applikationsdatenfeld
- Fig. 13 einen gemeinsamen Wertbereich (Cash Segment) als Applikationssegment im ADF
- Fig. 14 ein Beispiel der Datenorganisation mit gemeinsamem Wertbereich
- 15 Fig. 15 die Systemkompatibilität von segmentierten und nicht-segmentierten Identifikationsmedien
- Fig. 16 ein Beispiel einer Anlage mit mehreren unabhängigen Applikationen, mit mehreren Schreib- und Lesestationen und mehreren segmentierten Identifikationsmedien
- 20 Fig. 17 ein Anwendungsbeispiel einer Anlage an einem Ferienort mit mehreren unabhängigen Applikationen
- Fig. 18, 19 Beispiele von Identifikationsmedien, welche als Identifikationsträger an einem persönlichen Armband mitführbar sind.
- 25
- Figur 1 zeigt schematisch ein erfindungsgemässes Identifikationsmedium IM-S mit integriertem passivem Datenträger MI, dessen Betriebsenergie von der Schreib- und Lesestation WR ausgesendet und mittels einer HF-Antenne 45 aufgefangen wird. Der Datenträger MI weist einen hochintegrierten Spezialchip (ASIC) auf mit einem Prozessor 41, einem Datenspeicher 42 (z.B. in
- 30

Form eines EEPROM) sowie mit einer Steuerelektronik 43. Steuerelektronik und Prozessor steuern den gesamten externen und internen Datenaustausch, codieren die Sendedaten und decodieren die empfangenen Daten und enthalten den gesamten Hochfrequenzteil zur Speisung der Antenne 45  
5 inkl. Taktaufbereitung und Synchronisation für den Empfang von Energie und Daten der Sendestation WR.

Die Antenne 45 kann relativ grossflächig ausgebildet sein, wie in Figur 3b dargestellt ist, damit sich für alle Applikationen bzw. Applikationssegmente  
10 S1, S2, S3 gleichermassen eine relativ hohe Kommunikationsreichweite R ergibt.

Der Pfeil 20 illustriert die HF-Kommunikation mit der Schreib- und Lese-station WR (siehe Figur 2). Der Datenträger MI enthält ein unveränderbares Systemprogramm mit Sicherheitsfunktionen wie Prüfsummenkontrolle CRC  
15 und Verschlüsselungsalgorithmen 52. Der Datenspeicher 42 enthält dabei mehrere unabhängige Applikationssegmente S1, S2, S3 für frei verfügbare Anwendungen von unabhängigen Anwendern bzw. Lizenznehmern (SSC). Wie im folgenden weiter erläutert wird, weist der Speicher 42 eine Datenorganisa-tion auf mit einem gemeinsamen Datenfeld CDF, welches unveränderbare  
20 und nicht kopierbare Stammdaten mit einer Unikatsnummer 44 enthält, mit einem segmentierbaren Applikationsdatenfeld ADF, in welchem mehrere unabhängige Applikationen (App1, App2, App3) in Applikationssegmenten S1, S2, S3 einschreibbar sind, wobei jedes Applikationssegment eine Segment-kennung enthält. Dabei ist für alle Identifikationsmedien IM-S und alle zu-  
25 geordneten Schreib- und Lesestationen WR gültiges hierarchisches Autorisie-rungssystem A festgelegt, mit welchem jedes Identifikationsmedium IM-S initialisiert werden muss und mit welchem die gegenseitige Unbeeinflussbar-keit aller unabhängigen Applikationen mit deren Applikationssegmenten S1, S2, S3 sichergestellt ist. (Fig. 8, 10)

Dank diesem Aufbau ist der erfindungsgemässe Identifikationsträger bezüglich jeder Applikation weder auslesbar noch veränderbar und hardwaremässig auch nicht nachbaubar.

5

Figur 2 zeigt schematisch eine den Identifikationsmedien IM-S zugeordnete autonome und dezentral funktionsfähige Schreib- und Lesestation WR zur berührungslosen Kommunikation mit den Identifikationsmedien IM-S. Die Schreib- und Lesestation weist ein Sicherheitsmodul SM-S, eine separate Sende- und Empfangsantenne 54, eine Stromversorgung und eine zusätzliche Schnittstelle zu einem übergeordneten Rechner 75 auf. Das Sicherheitsmodul SM-S enthält alle Kommunikationsfunktionen mit den Datenträgern MI bzw. einem zugeordneten Applikationssegment des Identifikationsmediums. Dies umfasst die HF-Aufbereitung, die Verschlüsselung und Überprüfung der Daten auf korrekte Übertragung, die Prüfung der Lese- und Schreibberechtigung eines Identifikationsmediums bzw. Applikationssegments durch diese Schreib- und Lesestation sowie die Kommunikation mit einem übergeordneten Rechner. Die Sicherheitsfunktionen umfassen dabei Codieren und Decodieren der Daten, Identifizierung des Datenträgers MI und des betreffenden Applikationssegments, sowie Berechnung von Prüfsummen (CRC) zur fehlerfreien Datenübertragung. Der Kommunikationsablauf zwischen Identifikationsmedien IM-S und Schreib-Lesestationen WR wird später anhand von Figur 11 erläutert.

25

Die Figuren 3a und 3b zeigen in zwei Ansichten den Aufbau eines Identifikationsmediums IM-S mit einem Datenträger MI und mit einer Antenne 45. Diese Elemente sind vorzugsweise einstückig ausgebildet und dazu beispielsweise auf einer gedruckten Schaltung 46 angeordnet. Wie aus der Figur 3

30

ersichtlich ist, kann die Antennenfläche damit relativ gross ausgebildet sein, so dass für alle Applikationen und Applikationssegmente eines Identifikationsmediums IM-S besonders gute Kommunikationseigenschaften erreicht werden. Dies sind vor allem eine hohe Reichweite R bis zu mehreren Dezimetern und  
5 ein grosser Raumwinkelbereich W, in welchem die Kommunikation durchführbar ist, und eine weitgehende Unabhängigkeit von der relativen Positionierung des Identifikationsmediums und der zugeordneten Schreib- und Lese-  
station WR. Da mit einem einzigen erfindungsgemässen Identifikationsmedium IM-S viele bisherige einzelne Identifikationsmedien mit je nur einer Ap-  
10 plikation ersetzt werden, kann dieses Multi-Identifikationsmedium IM-S entsprechend aufwendiger aufgebaut sein, z.B. mit grösserer Antenne und weiteren, die Kommunikation und Reichweite verbessernden Eigenschaften. Überdies wird damit natürlich auch eine grosse Kosteneinsparung erreicht.

15 Die Figuren 4 bis 6 illustrieren die Datenorganisation des Speichers 42 der erfindungsgemässen segmentierten Identifikationsmedien IM-S. Vorzugsweise weist der veränderbare Speicher 42 als EEPROM mindestens 256 Byte Speicherplatz auf. Je nach Bedarf, d.h. entsprechend der Anzahl und Grösse der  
20 vorgesehenen Applikationssegmente S1, S2, S3 usw., welche in einem Identifikationsmedium IM-S untergebracht werden sollen, kann auch ein grösserer Speicher, z.B. mit 1 KByte, 4 KByte usw., eingesetzt sein. Die Speichergrösse jedes Applikationssegments ist mit Vorteil frei wählbar, so dass je nach Bedarf und bis zur Ausfüllung der gesamten Speicherkapazität eine Applikation  
25 nach der andern in ein Identifikationsmedium IM-S eingeschrieben werden kann.

Die Figur 4a zeigt eine Datenorganisation mit einem segmentierten Applikationsdatenfeld ADF, welches hier drei unterschiedlich grosse Applikations-  
30 segmente S1, S2, S3 aufweist. Diese drei Segmente entsprechen drei unabhän-



gigen Applikationen App1, App2, App3 von drei unabhängigen Anwendern oder Lizenznehmern mit Lizenznehmernummern SSC1, SSC2 und SSC3. Bei bisherigen, nicht-segmentierten Identifikationsmedien war für jede Applikation ein separates Medium IM1, IM2 und IM3 erforderlich.

5

Das Beispiel von Figur 4b zeigt eine Datenorganisation eines Identifikationsmediums IM-S, welche eine unabhängige Applikation App2 eines Lizenznehmers SSC2 aufweist, welche mehr als ein Applikationssegment (hier die Applikationssegmente S2.1 und S2.2) aufweist. Im Prinzip kann dabei der Lizenznehmer SSC2 im Rahmen der Applikation App2 auch gewisse Verbindungen zwischen den Segmenten S2.1 und S2.2 auf tieferem Organisationslevel OL2 festlegen. Dies wird später an den Figuren 7 bis 10 weiter erläutert. Auch hier sind jedoch die Applikationen App1, App2 und App3 vollständig unabhängig voneinander.

15

Figur 5 zeigt eine Datenorganisation eines Applikationssegments S1 mit einem Segment Header (Segmentkopf) SCDF1 und einem Applikationsdatenfeld SADF1. Im Segmentkopf SCDF sind für das betreffende Segment (S1) gültige Angaben und Bedingungen festgelegt. Das Datenfeld SADF1 ist für die Applikation frei verfügbar. Jedes Applikationssegment weist im Segment Header SCDF eine Anwendernummer SSC sowie Schreib- und Lesebedingungen für das Applikationssegment auf. Vorzugsweise werden dabei folgende Schreib- und Lesebedingungen festgelegt:

20 WRP = Write Protect, dies legt die Anzahl der schreibgeschützten Bytes im Speicher fest.

WRC = Write Condition, dies bestimmt, welche Schreib- und Lesestationen das Identifikationsmedium beschreiben und auch lesen dürfen. Dies sind nur Schreib- und Lesestationen, welche einen entsprechenden Taufdatensatz enthalten.

30

RD = Read Disable bedeutet einen Leseschutz, d.h. die Festlegung, wo der Datenträger gelesen werden darf und wo nicht.

Mit diesen Bedingungen legt jedes Identifikationsmedium IM-S selber fest, welche Stationen es lesen oder beschreiben dürfen. Jedes Applikationssegment enthält mit Vorteil auch eine Angabe der Segmentlänge LEN und eine  
5 Prüfsummenkontrolle CRC dieser Applikation.

Bei der Taufe einer den Identifikationsmedien IM-S zugeordneten Schreib- und Lesestation WR wird im Rahmen des Autorisierungssystems A durch ein  
10 spezielles Taufmedium ein Taufdatensatz in die Schreib- und Lesestation WR eingeschrieben, welcher die Berechtigung zur Bearbeitung eines Identifikationsmediums enthält, welches diesem Taufdatensatz entspricht. Jeder Taufdatensatz beginnt mit der Anwendernummer SSC, entsprechend der unabhängigen Applikation, und im speziellen legt der Taufdatensatz auch diese Lese-  
15 und Schreibbedingungen fest. Eine ungetaufte Schreib- und Lesestation WR kann also ein geschütztes Identifikationsmedium nicht lesen und beschreiben.

Figur 6 illustriert die Vererbung der Basisdatensätze (Stamp) eines jeden  
20 Segments, hier z.B. von Applikationssegment S1. Die Vererbung dieser Basisdaten wird an den folgenden Figuren 7 bis 9 genauer erläutert.

Diese zwangsweise Vererbung des Basisdatensatzes (Stamp) wird in Fig. 7  
25 weiter illustriert. Die Länge des vererbten Basisdatensatzes nimmt dabei proportional zum Organisationslevel OL zu. Hier nimmt z.B. der Basisdatensatz um 1 Byte zu, wenn der Organisationslevel OL um eine Stufe zunimmt, z.B. von OL2 zu OL3.

Die Figuren 7 bis 9 illustrieren das für alle Identifikationsmedien und alle zugeordneten Schreib- und Lesestationen des Systems gültige Autorisierungskonzept A mit hierarchischen Organisationslevels und der zwangsweisen Übertragung von Basisdatensätzen (Stamp), mit welchen die generelle Einhaltung der Systemregeln gesichert wird.

Die Figuren 8a, b illustrieren das hierarchische Autorisierungskonzept A, welches für alle Datenträger MI und für alle Schreib- und Lesestationen WR sowie für alle Autorisierungsdatenträger AMI und alle Programmierstationen WRI des Systems gültig ist und welches hierarchische Organisationsstufen oder Levels OL0, OL1, OL2, OL3, OL4 ... usw. aufweist.

Die höchste Stufe, der Organisationslevel OL0, entspricht dabei der Systemstufe, d.h. dem Inhaber oder Lizenzgeber 10 des ganzen Systems.

Die nächstuntere Stufe OL1 entspricht verschiedenen, unabhängigen Anwendern oder Lizenznehmern 101, 102, 103 usw. des Systems, z.B. verschiedenen Firmen, Gesellschaften, Gemeinden usw. Diese Stufe entspricht auch verschiedenen unabhängigen Applikationen, d.h. jedem unabhängigen Lizenznehmer und jeder unabhängigen Applikation ist eine SSC Nummer zugewiesen, welche diese von allen andern SSC Nummern unterscheidet.

Die nächstuntere Stufe OL2 entspricht verschiedenen Anwendungen 101.1, 101.2 eines Anwenders 101, z.B. verschiedenen Tochterfirmen einer Firma 101.

Die nächste Stufe OL3 entspricht verschiedenen Bereichen einer Anwendung, z.B. den Bereichen 101.11 der Tochterfirma 101.1 und den Bereichen 101.21, 101.22 der Tochterfirma 101.2.

Die nächste Stufe OL4 entspricht verschiedenen Unterbereichen von 101.21, 101.22 usw.

Mit diesem hierarchischen Autorisierungssystem wird sichergestellt, dass sich verschiedene unabhängige Applikationen App1, App2, App3, bzw. unabhängige Anwender 101, 102, 103 in keiner Weise gegenseitig beeinflussen können, wobei aber dennoch ein Anwender, z.B. 101, die Organisation in seinem Bereich, d.h. ab OL2, frei festlegen kann. Dies wird illustriert durch die Separationslinien 70 in Figur 8. Damit wird garantiert, dass auch von dieser Seite her kein Missbrauch irgendwelcher Art möglich ist, denn z.B. Applikationen von 101 sind in 102 und in 103 generell nicht zugelassen.

Mit jedem Schritt von einer Organisationsstufe nach unten von  $OL_n$  zu  $OL_{n+1}$  in diesem Autorisierungssystem werden die Befugnisse der Datenträger eingeschränkt, so dass sie nur nach unten, d.h. für Organisationsstufen mit höherer Nummer, Gültigkeit haben.

Dazu werden in die Applikationssegmente einer bestimmten Organisationsstufe immer alle fest vorgeschriebenen Daten der höheren Organisationsstufen zwangsweise eingeschrieben, also quasi vererbt, wie dies Figur 9 weiter illustriert. Für jede tiefere Organisationsstufe  $OL_{n+1}$  wird ein zusätzlicher Speicherteil im Speicher 42 fest beschrieben, wobei gleichzeitig alle Daten der höheren Organisationsstufe  $OL_n$  übernommen werden: es wird also nacheinander z.B. 10, 101, 101.1, 101.11 in die Speicherteile der Organisationsstufen OL0, OL1, OL2, OL3 eingeschrieben. Während, wie schon erläutert, bei bekannten bisherigen unsegmentierten Identifikationsmedien für jede unabhängige Applikation (101, 102, 103 usw.) ein eigenes Medium IM erforderlich war (Monomedien), ist es nun möglich, wie in Fig. 8b gezeigt ist, mehrere, beliebig wählbare unabhängige Applikationen auf nur einem einzigen Identifikationsmedium IM-S (Multimedium) zusammenzufassen. Dabei können z.B. mehr als 100 unabhängige Applikationen bzw. Lizenznehmernummern SSC bestehen und im segmentierten Identifikationsmedium IM-S ist es möglich, im Prinzip beliebig viele dieser unabhängigen Applikationssegmente aufzunehmen, soweit die Speicherkapazität des Mediums dies zulässt.

Dieses Autorisierungsprinzip wird noch verdeutlicht gemäss Figur 10, welche die Erzeugung bzw. Initialisierung von Identifikationsmedien mit Datenträgern MI illustriert. Alle Datenträger bzw. Identifikationsmedien des System müssen  
5 als Slavemedium 72 mittels eines Mastermediums 71 (als Autorisierungsdatenträger AMI) und einer speziellen Programmier-Schreib-Lesestation WRI erzeugt werden. Dabei wird auf ein neues, noch unbeschriebenes Identifikationsmedium bzw. auf ein Applikationssegment (hier z.B. auf S2) des Systems  
10 zwangsweise zusätzlich ein nicht löschbarer Basisdatensatz des Mastermediums 71 als Stamp für dies Applikation S2 auf das Slavemedium 72 übertragen, sozusagen vererbt oder eingeprägt. Dies geschieht nach den Regeln des hierarchischen Autorisierungssystems A. Dabei wird das erzeugte Identifikationsmedium (als Slavemedium 72) durch das Mastermedium 71 als Autorisierungsdatenträger AMI auch initialisiert. Diese Initialisierung ist Voraussetzung  
15 für die Zulassung zum Gebrauch des Applikationssegments S2 und des Identifikationsmediums IM-S im System. Nur initialisierte Identifikationsmedien und Applikationssegmente werden von den Schreib- und Lesestationen WR des Systems als gültig zugelassen. Dabei enthält jedes Autorisierungsmedium AMI eine Anwendernummer SSC, so dass es nur Applikationssegmente mit gleicher Anwendernummer SSC initialisieren und beschreiben kann.  
20

Figur 11 zeigt die Kommunikation 20 zwischen einer Schreib- und Lesestation WR mit Sicherheitsmodul SM-S und einem Datenträger MI bzw. einem Applikationsdatenfeld S2 des Identifikationsmediums IM-S. Dabei wird die notwendige elektromagnetische HF Feldenergie (z.B. mit einer Trägerfrequenz  
25 von 13 MHz) zusammen mit der aufmodulierten Information von der Schreib- und Lesestation WR an den Datenträger MI gesendet. Dort wird diese Feldenergie von der Antenne 45 aufgefangen und zum Betrieb des passiven Datenträgers MI sowie zum Senden der codierten Information an die WR einge-  
30

setzt. Eine besonders rationelle Ausführung dieser Informationsübertragung besteht darin, die Trägerfrequenz in einer Richtung, z.B. von der Schreib- und Lesestation WR zum Datenträger MI durch Pulsmodulation und in der Gegenrichtung (von MI zu WR) durch Belastungsmodulation zu modulieren.

- 5   Figur 11 illustriert nun einen abhörsicheren Ablauf dieser Kommunikation zwischen Schreib- und Lesestation WR und einem Applikationssegment S2 des Identifikationsmediums IM-S. Sobald ein Identifikationsmedium in das Feld einer Schreib- und Lesestation WR gelangt, beginnt automatisch der Ablauf zur Synchronisierung von WR und IM-S:
- 10   - bei jedem neuen Identifikationsvorgang werden von der Schreib- und Lesestation WR neue Initialisierungsdaten 51 (z.B. in Form von beliebigen Zufallszahlen) erzeugt und an das Identifikationsmedium gesendet (20.1).
- Hier erfolgt eine Verknüpfung dieser Initialisierungsdaten 51 mit einem fest gespeicherten Verschlüsselungscode (52) des Identifikationsmediums. Das
- 15   codierte Ergebnis (ein Schlüsselwort) wird dann an die Schreib- und Lesestation zurückgesendet (20.2),
- wo diese Information im Sicherheitsmodul SM-S entschlüsselt und geprüft wird (53), d.h. mit der in der WR ebenfalls gespeicherten Verschlüsselung (52) decodiert und mit den ursprünglichen, zufälligen Initialisierungsdaten 51
- 20   verglichen wird. An diesem Resultat kann die WR auch erkennen, um welche Art Medium es sich handelt.
- Anschliessend kann ohne Unterbruch eine synchronisierte Kommunikation (20.3) zwischen der Schreib- und Lesestation WR und dem Applikationssegment S2 des Identifikationsmediums IM-S stattfinden.
- 25   Mit dieser Methode werden die Taktgeneratoren und die Codegeneratoren von WR und IM-S synchronisiert. Nachdem ein Kommunikationsvorgang mit einem Applikationssegment abgeschlossen oder auch abgebrochen ist, muss jede neue Kommunikation (mit dem gleichen oder auch mit einem andern Applikationssegment) wieder mit neuen Initialisierungsdaten 51 beginnen.
- 30   Eine Aufzeichnung der übertragenen Daten und späteres Wiedereinspeisen ins

Feld ist dadurch nicht möglich, weil die ursprünglichen Initialisierungsdaten 51 nicht mehr gültig sind.

Somit ist es auch nicht möglich, Kopien von funktionsfähigen Identifikationsmedien zu erzeugen.

5

Zusätzlich werden die übertragenen Daten durch eine CRC-Überprüfung, d.h. durch eine Prüfsummenkontrolle, bei der z.B. Nutzdaten mit Stammdaten des Datenträgers MI verknüpft werden, überprüft. Damit werden fehlerhafte Datenübertragungen praktisch ausgeschlossen. Dies ist vor allem wichtig, wenn sensible Daten oder Wertänderungen von einer autorisierten Schreib- und Lesestation in ein Applikationssegment eingeschrieben werden, wobei neu eingeschriebene Daten überprüft werden, bevor sie Gültigkeit erhalten. Mit diesem Kommunikationsablauf wird somit sichergestellt, dass kein Abhören der Kommunikation zur Herstellung gefälschter Applikationssegmente auf den Identifikationsmedien missbraucht werden kann.

Figur 12 zeigt als weiteres wichtiges Sicherheitselement einen Schattenspeicher (shadow memory) im Applikationsspeicher ADF. Wenn ein Kommunikationsvorgang zwischen Identifikationsmedium IM-S und Schreib- und Lesestation WR gestört oder unterbrochen wird, bei dem neue sensible Daten in den Datenträger eingeschrieben werden, so ist es wichtig, dass dabei keine sensiblen Daten verloren gehen oder unerwünscht verändert werden. Ein solcher Kommunikationsvorgang mit sensiblen Daten sollte daher entweder vollständig und richtig ausgeführt werden oder ein unvollständiger oder unrichtiger Datentransfer sollte als Ganzes gestrichen werden. Eine solche Störung oder Unterbrechung eines Kommunikationsvorgangs kann vor allem auftreten, wenn sich das Identifikationsmedium während des Kommunikationsvorgangs aus dem Sendebereich R der Schreib- und Lesestation entfernt.

Mittels eines Schattenspeichers *shad* im Identifikationsmedium wird nun erreicht, dass jeder Kommunikationsvorgang entweder vollständig oder gar nicht eingeschrieben wird. Dabei werden zuerst die alten Daten im ADF, bzw. in einem Segment, in den Schattenspeicher übertragen und kontrolliert. Wenn  
5 die alten Daten korrekt im Schattenspeicher vorhanden sind, werden die neuen Daten von der Schreib- und Lese- station ins Applikationssegment übertragen und dort kontrolliert. Falls diese übertragenen neuen Daten vollständig und richtig sind, bleiben sie als gültig im Applikationssegment.  
Falls die neuen Daten nicht vollständig und richtig übertragen wurden, werden  
10 alle neuen Daten im Applikationssegment gelöscht und es werden wieder die alten Daten aus dem Schattenspeicher ins Applikationssegment zurückgeschrieben.  
Anschliessend kann der Kommunikationsvorgang in der gleichen Weise wiederholt werden, bis die neuen Daten korrekt und vollständig im Applikations-  
15 segment des Identifikationsmediums eingeschrieben sind.

Figur 13 zeigt als wichtiges Anwendungsbeispiel einen gemeinsamen Wertbereich als Applikationssegment *Scash* im Identifikationsmedium auf welchen  
20 andere berechnigte Applikationssegmente (S1, S2, S3) Zugriff haben. Der Zugriff aus den Applikationssegmenten erfolgt über einen Systemcode in einem Referenzbereich *Ref*. Jedes Segment weist ebenfalls einen Segment-Referenzbereich *Ref1*, *Ref2*, *Ref3* auf. Damit kann das gemeinsame *Cash*segment *Scash* an einer zugeordneten Schreib- und Lese- station als Geldauflade-  
25 station entsprechend einem einbezählten Betrag aufgeladen werden. Dieser gutgeschriebene Betrag auf dem Identifikationsmedium IM-S kann an verschiedenen Stationen der Applikationssegmenten S1, S2 usw. sukzessive verbraucht werden. Dabei werden die einzelnen Bezüge jeweils den entsprechenden Applikationssegmenten S1, S2 usw. belastet. Den Abbuchungen auf Seite



des Identifikationsmediums IM-S entspricht so die Verrechnung auf Seite der Applikationsstationen WR.

- 5    Figur 14 zeigt ein Ausführungsbeispiel einer Datenorganisation eines gemeinsamen Teilsegment Scash mit einem Segmentkopf SCDF, einem Referenzbereich mit einem Systemcode SC, einem Schattenspeicher shad, dem Wertbereich cash sowie mit Prüfsummenkontrollen CRC über diese Bereiche.

10

- Figur 15 illustriert die Systemkompatibilität von segmentierten Identifikationsmedien IM-S (multi) und nicht-segmentierten Identifikationsmedien IM (mono) bezüglich der zugeordneten Schreib- und Lesestation WR mit entsprechenden Sicherheitsmodulen SM-S (multi) und SM (mono) sowie auch mit  
15    den zugeordneten Programmier-Schreib- und Lesestationen WRI mit Sicherheitsmodulen MSM-S (multi) und MSM (mono). Wie die Figur zeigt, ist das System aufwärtskompatibel, d.h. mono Identifikationsmedien können zusätzlich auch von segmentierten Sicherheitsmodulen SM-S der Schreib- und Lesestationen und Sicherheitsmodulen MSM-S der Programmierstationen bearbeitet bzw. erstellt werden. Somit können in einer Anlage mit segmentierten  
20    Medien IM-S auch unsegmentierte Medien IM eingesetzt werden. Oder eine bestehende Anlage mit mono Medien kann zusätzlich auch mit multi Medien IM-S aufgerüstet werden. Die Sicherung dieser Kompatibilität erfolgt durch die Datenorganisation im Systemdatenfeld SDF der segmentierten Identifikationsmedien IM-S.  
25

- Figur 16 illustriert schematisch eine Anlage, welche mehrere unabhängige Applikationen aufweist, hier mit segmentierten Identifikationsmedien IM-S,  
30    welche beliebige verschiedene Kombinationen von Applikationssegmenten von

S1 bis S20 aufweisen. Die unabhängigen Applikationen App1 bis App20 entsprechen den unabhängigen Lizenznehmern oder Anwendern mit Nummern SSC1 bis SSC20 und diese entsprechen den Applikationssegmenten S1 bis S20. Die zugeordneten dezentralen und autonom funktionsfähigen Schreib- und Lesestationen WR weisen Taufdatensätze für eine oder mehrere Applika-  
5 tionen S1 bis S20 auf. Die Schreib- und Lesestationen WR sind zusätzlich an einen übergeordneten Hostcomputer 75 anschliessbar. In dieser Anlage sind auch nicht-segmentierte Identifikationsmedien IM einbezogen, wie das Beispiel mit S20 zeigt. Dies entspricht der Systemkompatibilität gemäss Figur 15.

10

Figur 17 zeigt als Beispiel eine Anlage in einem geografischen Gebiet, z.B. in einer Ferienregion, mit den unabhängigen Anwendern SSC1 bis SSC5 mit den entsprechenden unabhängigen Applikationen und Applikationssegmenten S1  
15 bis S5. Die Applikationen S1 und S2 seien zwei verschiedene Bergbahn- und Skiliftgebiete, welche von den entsprechenden Bahnbetriebsgesellschaften als Anwender SSC1 und SSC2 geführt werden.

Die Applikation S3 sei ein öffentlicher Bus, Schwimmbad und Sportanlagen, Parkgaragen und ein Hotel, welche von der Ortsgemeinde als SSC3 geführt  
20 werden.

Die Applikation S4 seien verschiedene Einkaufsläden, welche von einem Zusammenschluss einiger Geschäftsinhaber als Anwender SSC4 geführt werden.

Die Applikation S5 seien Telefon- und Postdienste, welche von der PTT als  
25 Anwender SSC5 geführt werden.

Das Applikationssegment S5 verfügt über einen eigenen Cashbereich, während die Segmente S1 bis S4 über ein gemeinsames Cashsegment Scash verfügen.

Hier kann ein erfindungsgemäss segmentiertes Identifikationsmedium IM-S im  
30 Prinzip beliebige Kombinationen von Segmenten S1 bis S5 aufweisen, wobei

auch die einzelnen Segmente entsprechend der Festlegung des entsprechenden Anwenders in sich wiederum frei strukturiert werden können (siehe Figur 8).

- 5 Ein weiteres Beispiel ist eine Anlage mit verschiedenen Firmen als unabhängige Anwender. Dabei können Applikationssegmente je einer Firma, bzw. ihrem Personal, zur Verfügung stehen. Andere Applikationssegmente können von zwei oder mehreren Firmen gemeinsam betrieben werden, z.B. für gemeinsame Infrastruktur und Einrichtungen, und weitere Applikationssegmente
- 10 können neben Firmenangehörigen auch Aussenstehenden zur Verfügung stehen, z.B. ein Personalrestaurant oder ein Schwimmbad, wobei auch unterschiedliche Benützungspreise für verschiedene Benutzer vorgegeben werden können.
- 15
- Das Identifikationsmedium kann zusätzlich noch mit einer persönlichen Codierungsfunktion kombiniert sein, um besonders hohen Sicherheitsanforderungen in bestimmten Anwendungen genügen zu können. Dazu können z.B. ein PIN Code oder biometrische Datencodes eingesetzt werden. Persönliche
- 20 biometrische Daten werden z.B. aus Fingerabdrücken oder Finger-, Hand- und Kopfgeometrien ermittelt und mit den entsprechenden im Datenträger MI gespeicherten Codes 33 (Fig. 1, 3b, 18b) verglichen zwecks persönlicher Identifikation und Verifikation eines berechtigten Trägers.
- 25 Die Identifikationsmedien IM-S können in verschiedenen an sich bekannten Formen realisiert sein, meist z.B. als Karten. Sie können aber auch mit einem anderen Element kombiniert werden, z.B. mit einem persönlichen Gegenstand, etwa einem Armband, welches von einer Person immer mitgeführt wird. Durch diese Kombination bzw. Verbindung von Identifikationsmedium und
- 30 mitgeführtem persönlichen Gegenstand wird sichergestellt, dass das Identifika-

tionsmedium immer mitgeführt wird und damit der berechtigten Person auch immer zur Verfügung steht, wenn es gebraucht wird. Karten demgegenüber können auch in Kleidertaschen vergessen werden.

5

Figur 18 zeigt ein Beispiel eines mitführbaren Identifikationsträgers 1 als Identifikationsmedium IM-S in zwei Ansichten 18a, 18b. Der Identifikationsträger ist an einem persönlichen Armband PA, welches am Arm 11 getragen wird, in einer geeigneten Position auswechselbar befestigt. Der Identifikationsträger besteht aus einem separaten, flachen Trägerelement 1 und einer lös-  
10 baren Befestigungsvorrichtung 3, welche ein Auswechseln des persönlichen Armbands PA ermöglicht. Das Trägerelement 1 enthält den passiven integrierten elektronischen Datenträger MI mit Prozessor, elektrischer Schaltung und Datenspeicher sowie eine Antenne 45, welche von einem Dielektrikum 4,  
15 hier beidseitig von einer dielektrischen Überdeckungsschicht, umgeben ist. Die Antenne 45 (hier in Form einer Antennenschlaufe) weist mindestens teilweise offene Antennen-Abstrahlflächen FAO auf, welche nicht von elektrisch leitenden Teilen bzw. von elektromagnetisch undurchlässigem Material des persönlichen Armbands abgedeckt sind. Eine Illustration dazu findet sich  
20 im Beispiel von Figur 19. Zwecks optimaler Anpassung an die Rundung des Arms 11 und des Armbands kann der Datenträger leicht gebogen ausgeführt und mit Vorteil aus einem flexiblen Material z.B. aus Kuststoff aufgebaut sein. Die Befestigungsvorrichtung 3 ist hier einstückig mit dem Trägerelement 1 verbunden, und sie besteht z.B. aus einem oder zwei Bändern 8 mit je ge-  
25 genüberliegenden, miteinander verbindbaren Enden. Das Trägerelement 1 ist hier unter dem Armband PA liegend, d.h. zwischen Arm 11 und Armband angebracht. Die Enden von 8 umschliessen dabei das Armband PA, so dass sie dem Arm 11 gegenüberliegend über dem Armband PA zusammen geschlossen werden. Die Länge dieses Verschlusses ist dabei so verstellbar, dass  
30 er unterschiedliche Querschnittsumfängen des persönlichen Armbands PA

optimal angepasst werden kann. Dazu sind z.B. formschlüssige Verschlusselemente auf den Enden von 8 angeordnet (Fig. 19).

Die Figuren 18a, b illustrieren ein Beispiel von Befestigungsvorrichtungen mit Klettverschlüssen 15 an beiden Bandenden eines breiten zentralen Bandes 8. Auf einem Bandende ist der Schlaufenteil 15.2 des Klettverschlusses angebracht und das Gegenstück, der Hakenteil 15.1, befindet sich auf dem andern Bandende. Die Länge dieser beiden Klettverschlussteile 15.1 und 15.2 ist dabei so gewählt, dass eine maximale Längenänderung DL des Verschlusses - in Anpassung an verschieden grosse persönliche Armbänder PA - erreicht werden kann. Mit dem Klettverschluss ist ein besonders einfaches und praktisches Auswechseln des persönlichen Armbands PA möglich. Bei geeigneter Auslegung bezüglich Material und Lage der beiden Klettverschlussteile 15.1 und 15.2 ist ein sicherer, wenig auftragender Verschluss realisierbar, welcher sich unter normalen Behandlungsbedingungen nicht öffnet.

In der Ansicht von Figur 18b, im Querschnitt zum persönlichen Armband PA, ist der Aufbau des Trägerelements dargestellt mit einem Datenträger MI sowie mit einer flachen Antenne 45, welche beispielsweise als Luftschleife auf einer gedruckten Schaltung aufgebracht sein kann. Beidseitig der Antenne ist eine Überdeckung mit einem Dielektrikum 4 angebracht, welche eine Dicke D1 von z.B. vorzugsweise mindestens 0.5 mm aufweist und welche beispielsweise 0.5 bis 1 mm betragen kann.

In einer anderen Ausführung kann das Trägerelement 1 z.B. zusammen mit der Befestigungsvorrichtung 3 als elastischer Bügel eine das Armband PA umfassende Klammer bilden. Eine weitere Variante bildet eine Befestigungsart mittels vier elastischer Lappen, welche als Befestigungsvorrichtung an den Ecken des Trägerelements angebaut sind und welche an das persönliche Armband PA aufsteckbar sind. Das Trägerelement 1 und die Befestigungsvorrichtung

tung 3 können auch als zwei separierbare und fest zusammenfügbare Teile ausgebildet sein. Eine weitere Ausführungsvariante bilden Ferrit-Antennen anstelle von Schlaufenantennen, z.B. als flacher Ferrit-Stab mit elektrischer Wicklung, dessen Achse parallel zum Unterarm 11 verläuft.

5

Es sind verschiedene Positionen bezüglich des Armbands PA möglich: Das Trägerelement 1 kann unter dem Armband, oben auf dem Armband oder seitlich neben dem Armband angeordnet sein.

- 10 Die Figur 19 zeigt ein Beispiel mit einer Armanduhr 21 als persönliches Armband PA, wobei das Trägerelement 1 unter dem Armband und neben der Uhr 22 angeordnet und mit einem Band 8 als Befestigungsvorrichtung fixiert ist. Auch hier ergeben sich relativ grosse, nicht vom Armband PA abgedeckte offene Antennen-Abstrahlflächen FAO.

**Bezeichnungsliste P1087**

	1	Trägerelement
5	3	Befestigungsvorrichtung
	4	Dielektrikum, Abdeckung
	5	Verschluss von 3
	8	Bänder von 3
	10	Systeminhaber, Lizenzgeber
10	101, 102	unabhängige Anwender, Lizenznehmer
	101.1, 101.2	Anwendungen von 101
	11	Arm, Handgelenk
	15	Klettverschluss
15	15.1	Hakenteil
	15.2	Schlaufenteil
	20	Kommunikation HF-Signale
	20.1, 20.2,	
	20.3	Kommunikationsablauf
20		
	21	Armbanduhr
	22	Uhr
	33	persönliche biometrische Codierungsfunktionen
	41	Prozessor
25	42	Speicher
	43	Steuerelektronik
	44	Stammdaten mit Unikatsnummer
	45	Antenne
	46	gedruckte Schaltung (IC) Chip
30	51	Initialisierungsdaten (Zufallszahlen)

- 22 -

	52	Verschlüsselungscode in MI
	53	Entschlüsselung in WR
	54	Antenne WR
	70	Separationslinie
5	71	Mastermedium
	72	Slavemedium
	75	übergeordneter Rechner
10	App1, App2	unabhängige Applikationen (SSC)
	MI	Datenträger
	AMI	Autorisierungsdatenträger
	WR	Schreib- und Lesestation
	WRI	Programmier-Schreib-Lesestation
15	CRC	Prüfsummenkontrolle
	A	Autorisierungssystem
	OL0, OL1,	
	OL2	Organisationslevel
20	W	Raumwinkelbereich für Kommunikation
	R	Kommunikationsreichweite
	IM	Identifikationsmedium (mono) nicht-segmentiert
	IM-S	Identifikationsmedium (multi) segmentiert
	SM	Sicherheitsmodul von WR (mono)
25	SM-S	Sicherheitsmodul von WR (multi) segmentiert
	MSM	Sicherheitsmodul von WRI (mono)
	MSM-S	Sicherheitsmodul von WRI (multi)
	S1, S2, S3	Applikationssegmente
	CDF	gemeinsames Datenfeld
30	SDF	Systemdatenfeld



	ADF	Applikationsdatenfeld
	SCDF	Segmentkopf (Segment Header)
	SADF	Segment-Applikationsdatenfeld
	SSC	Anwendernummer, Lizenznehmernummer
5	WRP	Schreibschutz
	WRC	Schreibbedingungen
	RD	Leseschutz
	LEN	Segmentlänge
	Scash	gemeinsames Wertsegment
10	cash	Wertbereich, Wertsegment
	Ref	Referenz Wertbereich
	shad	Schattenspeicher (shadow memory)
	SC	Systemcode
		Taufdatensatz
15		
	D1	Dicke von 4
	DL	Längenänderung von 3
	FAO	offene Antennen-Abstrahlflächen
	PA	persönliches Armband
20		

## PATENTANSPRÜCHE

5

1. Identifikationsmedium mit passivem elektronischem Datenträger MI,  
welcher einen Prozessor, eine Steuerelektronik und einen Speicher sowie  
eine Antenne zur berührungslosen Übertragung von HF-Signalen als  
codierte Kommunikation an eine zugeordnete Schreib- und Lesestation  
10 WR aufweist,  
dadurch gekennzeichnet, dass der Speicher (42) eine Datenorganisation  
aufweist mit  
einem gemeinsamen Datenfeld CDF, welches unveränderbare und nicht  
kopierbare Stammdaten mit einer Unikatsnummer (44) enthält,  
15 mit einem segmentierbaren Applikationsdatenfeld ADF, in welchem  
mehrere unabhängige Applikationen (App1, App2, App3) in Applika-  
tionssegmenten (S1, S2, S3) einschreibbar sind,  
wobei jedes Applikationssegment eine Segmentkennung enthält und wo-  
bei ein für alle Identifikationsmedien IM-S und alle zugeordneten  
20 Schreib- und Lesestationen WR gültiges hierarchisches Autorisierungs-  
system A festgelegt ist, mit welchem jedes Identifikationsmedium IM-S  
initialisiert werden muss und mit welchem die gegenseitige Unbeeinfluss-  
barkeit aller unabhängigen Applikationen mit deren Applikationssegmen-  
ten (S1, S2, S3) sichergestellt ist.  
25
2. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass  
der Speicher auch ein Systemdatenfeld SDF enthält mit Daten zur Siche-  
rung der Systemkompatibilität mit nicht-segmentierten Identifikations-  
30 medien IM des gleichen Systems.

3. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass jedes Applikationssegment (S1, S2, S3) einen Segment Header (Segmentkopf) SCDF aufweist, in welchem für das betreffende Segment gültige Angaben und Bedingungen festgelegt sind sowie ein für die Applikation frei verfügbares Datenfeld SADF aufweist.
4. Identifikationsmedium nach Anspruch 3, dadurch gekennzeichnet, dass jedes Applikationssegment im Segment Header SCDF eine Anwendernummer SSC sowie Schreib- und Lesebedingungen für das Applikationssegment enthält.
5. Identifikationsmedium nach Anspruch 4, dadurch gekennzeichnet, dass jedes Applikationssegment folgende Schreib- und Lesebedingungen enthält: WRP = (Write Protect) Schreibschutz, WRC (Write Condition) = Schreibbedingungen und RD = Leseschutz.
6. Identifikationsmedium nach Anspruch 3, dadurch gekennzeichnet, dass jedes Applikationssegment zusätzlich die Segmentlänge LEN und eine Prüfsummenkontrolle CRC dieser Applikation enthält.
7. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass die Speichergrösse jedes Applikationssegments (S1, S2, S3) frei wählbar ist. (nach Bedarf und Speichergrösse)

8. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass mindestens eine unabhängige Applikation (App2) mehr als ein Applikationssegment (S2.1, S2.2, S2.3) aufweist.

5

9. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass zur Kommunikation zwischen Identifikationsmedium IM-S und Schreib- und Lesestation WR bei jedem Identifikationsvorgang von der Schreib- und Lesestation WR neue Initialisierungsdaten (51) mit Zufallszahlen erzeugt und an das Identifikationsmedium IM-S gesendet werden (20.1), welche dort mit einem fest gespeicherten Verschlüsselungscode (52) des Identifikationsmediums verknüpft und in dieser codierten Form an die Schreib- und Lesestation zurückgesendet werden (20.2), wo diese Information in einem Sicherheitsmodul SM-S der Schreib- und Lesestation WR entschlüsselt und geprüft wird (53) und worauf anschliessend eine synchronisierte Kommunikation (20.3) zwischen der Schreib- und Lesestation WR und dem Identifikationsmedium IM-S stattfindet.

10. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass die Kommunikation von der Schreib- und Lesestation WR immer nur mit einem einzigen Identifikationsmedium IM-S erfolgt und dass keine Kommunikation erfolgt, wenn sich gleichzeitig mehr als ein Identifikationsmedium im Sendebereich R der Schreib- und Lesestation WR befindet.

11. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass das Identifikationsmedium bzw. der Datenträger MI einen ver-

änderbaren Speicher (EEPROM) mit mindestens 256 Byte Speicherplatz aufweist.

- 5      12.      Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass Antenne und Datenträger einstückig ausgebildet und auf einer gedruckten ASIC Schaltung (46) angeordnet sind.
- 10      13.      Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass im Applikationsdatenfeld ADF ein Schattenspeicher shad vorhanden ist, in welchen während eines Schreibvorgangs mit sensiblen Daten diese Daten zwischengespeichert werden, so dass der Schreibvorgang immer entweder vollständig richtig oder gar nicht ausgeführt wird.
- 15
14.      Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass im Applikationsdatenfeld ADF veränderbare Wertbereiche cash enthalten sind, welche von autorisierten Schreib- und Lesestationen beschreibbar sind.
- 20
15.      Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass im Applikationsdatenfeld ADF ein gemeinsamer Wertbereich cash als Applikationssegment Scash vorhanden ist, auf welchen andere berechnigte Applikationssegmente (S1, S2, S3) Zugriff haben.
- 25

16. Identifikationsmedium nach Anspruch 1, dadurch gekennzeichnet, dass der Datenträger MI eine zusätzliche persönliche Codierungsfunktion (33) enthält, wie einen PIN Code oder einen biometrischen Datencode.

5

17. Anlage mit mehreren Identifikationsmedien nach Anspruch 1 für mehrere unabhängige Applikationen (App1, App2, App3) von mehreren unabhängigen Anwendern (SSC) mit mehreren zugeordneten autonomen dezentralen Schreib- und Lesestationen WR für diese Applikationen, wobei die Identifikationsmedien IM-S verschiedene Kombinationen von Applikationssegmenten (S1, S2, S3) aufweisen und wobei die Schreib- und Lesestationen WR an einen übergeordneten Host-Computer (75) anschliessbar sind.

15

18. Anlage nach Anspruch 17, dadurch gekennzeichnet, dass im Rahmen des gleichen Autorisierungssystems A zusätzlich nicht-segmentierte Identifikationsmedien IM von je nur einem unabhängigen Anwender (SSC) vorhanden sind, welche von allen autorisierten - segmentierten (SM-S) und nicht-segmentierten (SM) - Schreib- und Lesestationen WR bearbeitbar sind.

20

19. Anlage nach Anspruch 17, dadurch gekennzeichnet, dass sie in einem Feriengebiet mehrere unabhängige Applikationen umfasst für Freizeit- und Sportanlagen, Schwimmbad, Bergbahnen und Skilifte, Restaurants, Parkgaragen, öffentliche Verkehrsmittel, Getränke- und Nahrungsmittelautomaten, Einkaufsläden und Telefon.

25

30

20. Verfahren zur Initialisierung eines Identifikationsmediums nach Anspruch  
1 im Rahmen des hierarchischen Autorisierungssystems A, dadurch ge-  
kennzeichnet, dass jedes Identifikationsmedium IM-S mittels eines spe-  
ziellen Autorisierungsmediums AMI und einer speziellen Programmier-  
5 Schreib-Lesestation WRI initialisiert werden muss.
21. Verfahren nach Anspruch 20, dadurch gekennzeichnet, dass jedes Identifi-  
kationsmedium IM-S, IM des Systems als Slavemedium (72) mittels eines  
10 übergeordneten Autorisierungsmediums AMI als Mastermedium (71)  
erzeugt werden muss, wobei zwangsweise ein nicht mehr veränderbarer  
Basisdatensatz des Mastermediums als Stamp auf das Slavemedium über-  
tragen (vererbt) wird.
- 15 22. Verfahren nach Anspruch 21, dadurch gekennzeichnet, dass die Länge  
des vererbten Basisdatensatzes (Stamp) proportional zum Organi-  
sationslevel OL zunimmt, z.B. um ein Byte wenn der Organisations-  
level OL um eine Stufe zunimmt.
- 20 23. Verfahren nach Anspruch 20, dadurch gekennzeichnet, dass jedes  
Autorisierungsmedium AMI immer nur eine Anwendernummer SSC  
enthält und dass es nur Applikationssegmente (S1, S2, S3) mit glei-  
25 cher Anwendernummer SSC initialisieren und beschreiben kann.
24. Verfahren zur Taufe einer den Identifikationsmedien nach Anspruch  
1 zugeordneten Schreib- und Lesestation WR im Rahmen des Autori-  
30 sierungssystems A, dadurch gekennzeichnet, dass durch ein spezielles

Taufmedium ein Taufdatensatz in die Schreib- und Lese- station WR eingeschrieben wird, welcher die Berechtigung zur Bearbeitung von dem Taufdatensatz entsprechenden Identifikationsmedien IM-S ergibt.

5

25. Identifikationsmedium nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass das Identifikationsmedium IM-S als von einer Person mitführbarer berührungsloser Identifikationsträger mit Zutrittsfunktionen ausgebildet ist und dass der Identifikationsträger als separates, flaches Trägerelement (1) an einem persönlichen Armband PA mittragbar und auswechselbar befestigt ist, und wobei das Trägerelement (1) den passiven integrierten elektronischen Datenträger MI mit Prozessor, elektrischer Schaltung und Speicher sowie eine integrierte Antenne (45) und eine lösbare Befestigungsvorrichtung (3) aufweist und wobei die Antenne von einem Dielektrikum (4) umgeben ist und mindestens teilweise offene Abstrahlflächen FAO aufweist, welche nicht durch elektrisch leitende Teile des persönlichen Armbands PA abgedeckt sind.

20

26. Identifikationsmedium nach Anspruch 25, dadurch gekennzeichnet, dass das persönliche Armband PA eine Armbanduhr (21) ist und das Trägerelement (1) so befestigbar ist, dass offene Antennen-Abstrahlflächen FAO vorhanden sind, welche nicht überdeckt werden.

25

27. Identifikationsmedium nach Anspruch 25, dadurch gekennzeichnet, dass die Befestigungsvorrichtung (3) einen Klettverschluss (15) oder einen Schnappverschluss aufweist.

30



1/11

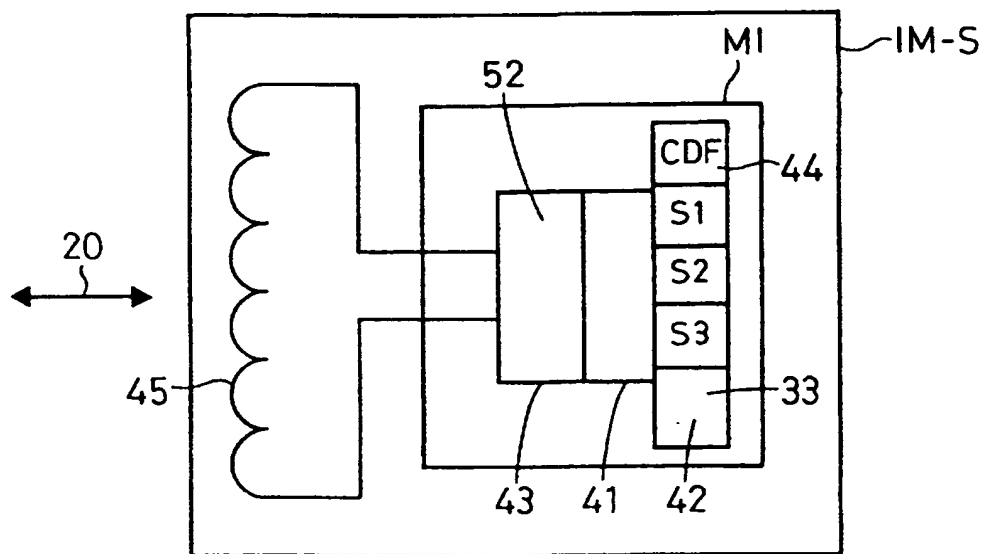


FIG. 1

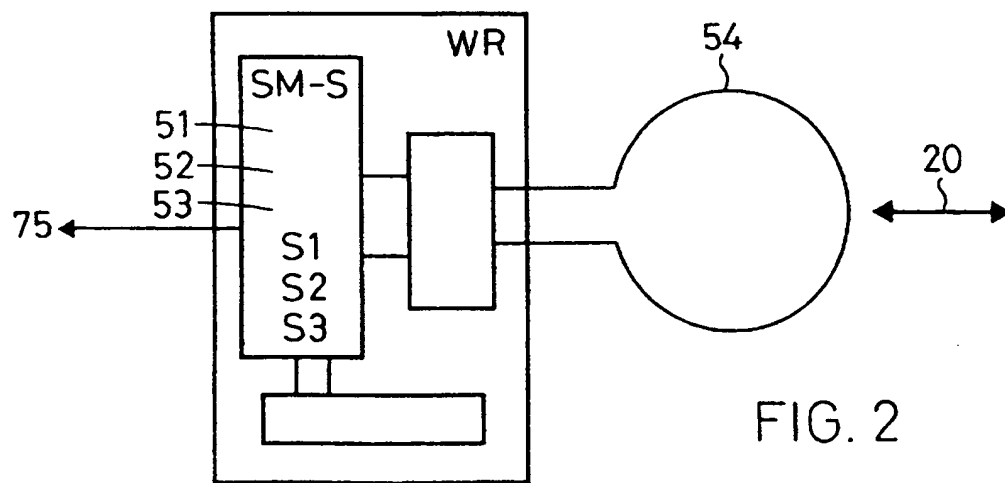


FIG. 2

2/11

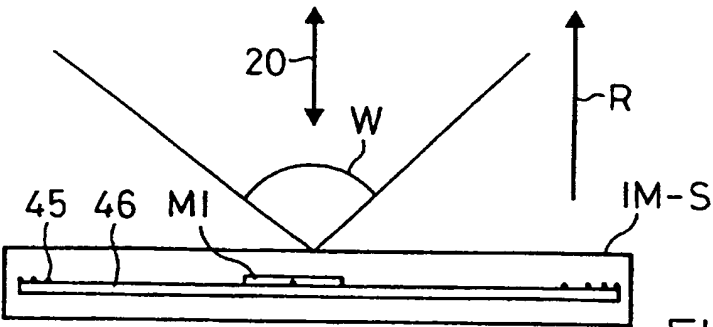


FIG. 3a

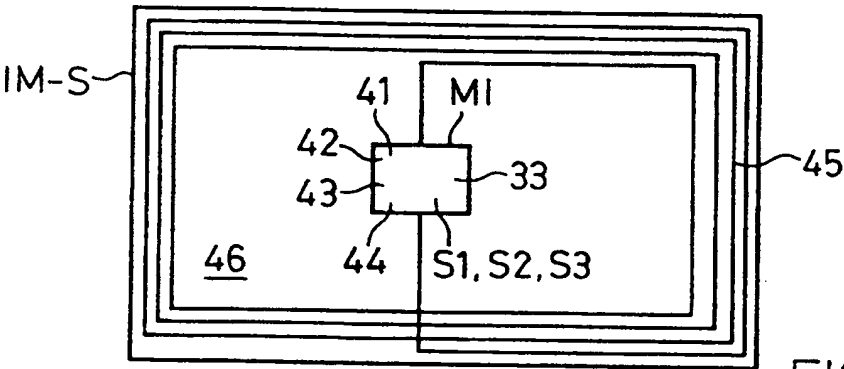


FIG. 3b

	Byte 1	Byte 2	Byte 3	Byte 4	
OL 0					System
OL 1	SSC				Applicant
OL 2	SSC				
OL 3	SSC				
OL 4	SSC				
OL~Stamp					
Stamp					

FIG. 7

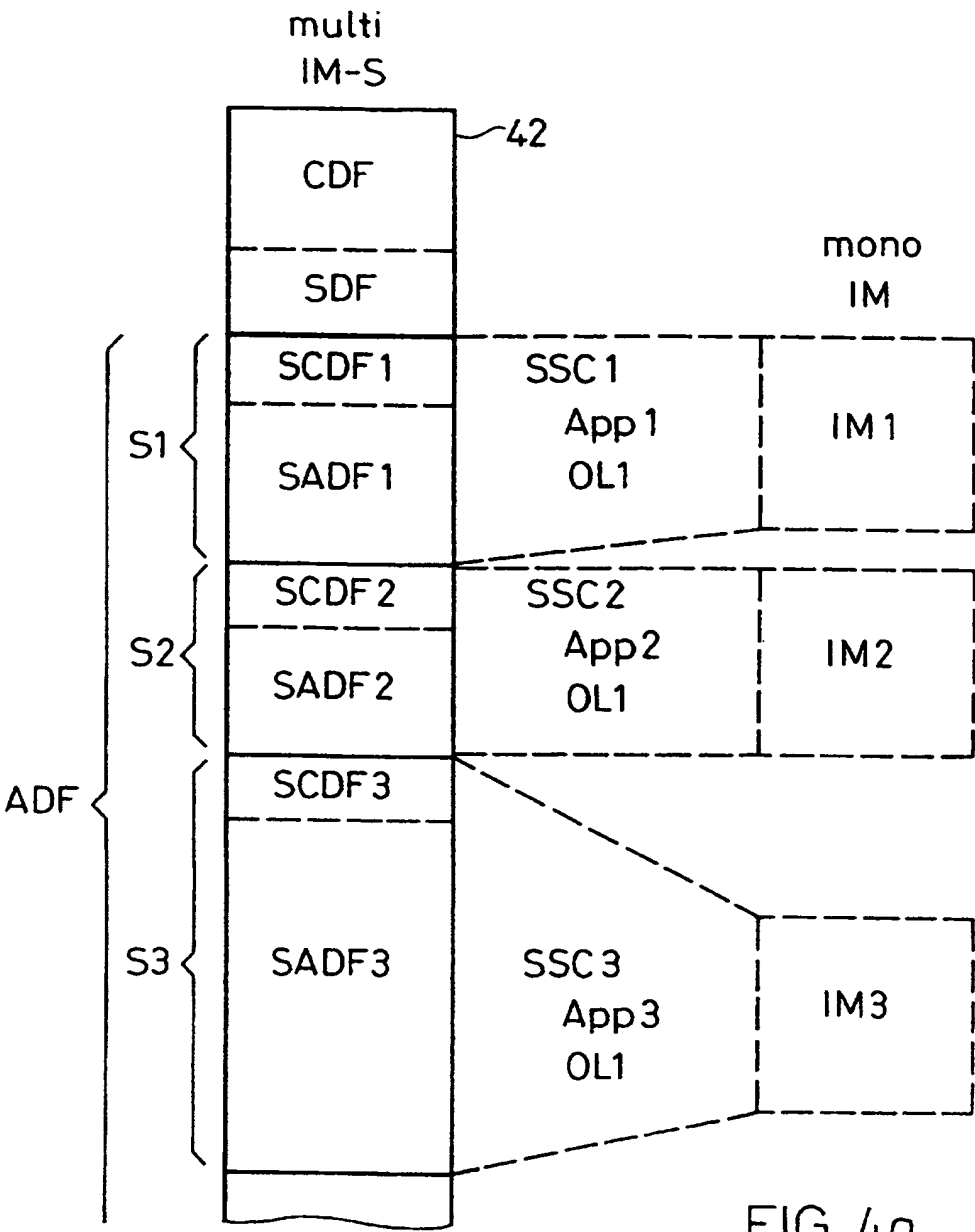


FIG. 4a

4/11

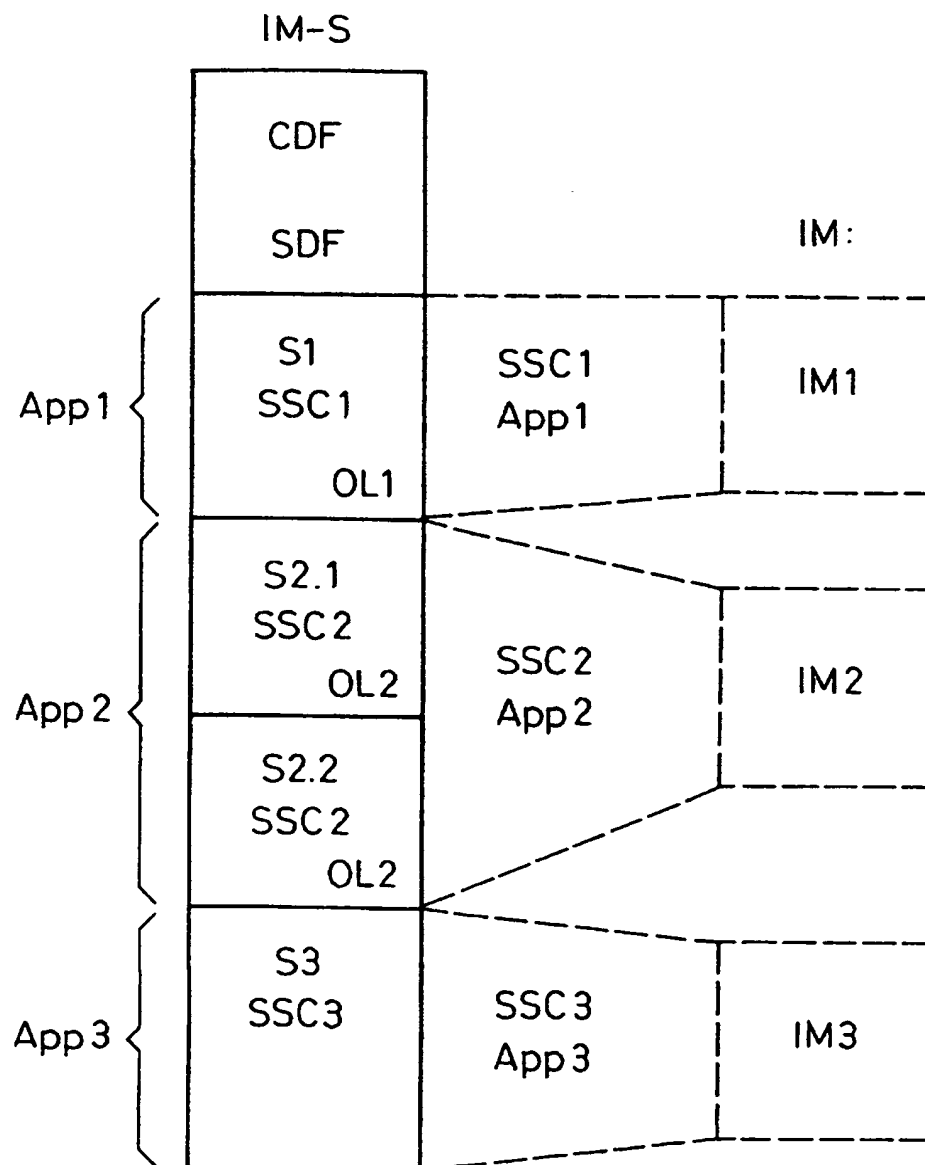


FIG. 4b

5/11

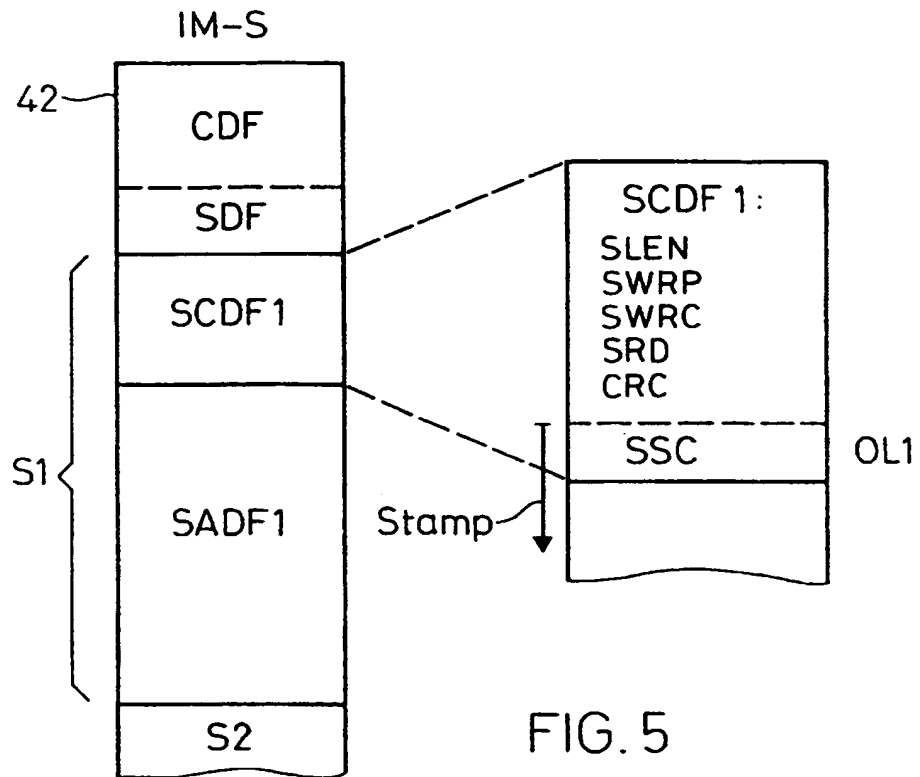


FIG. 5

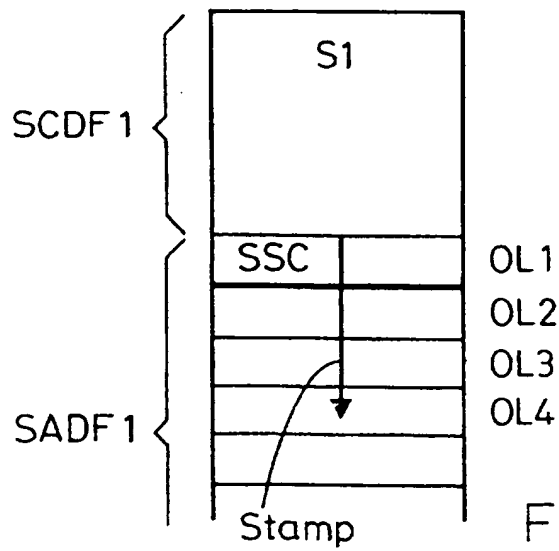
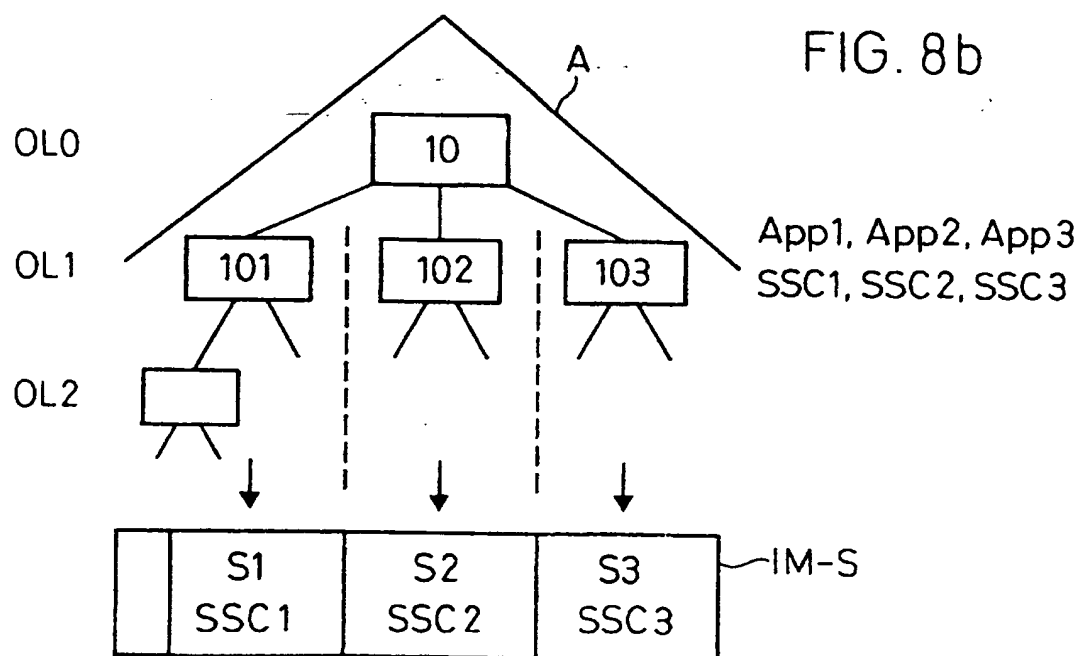
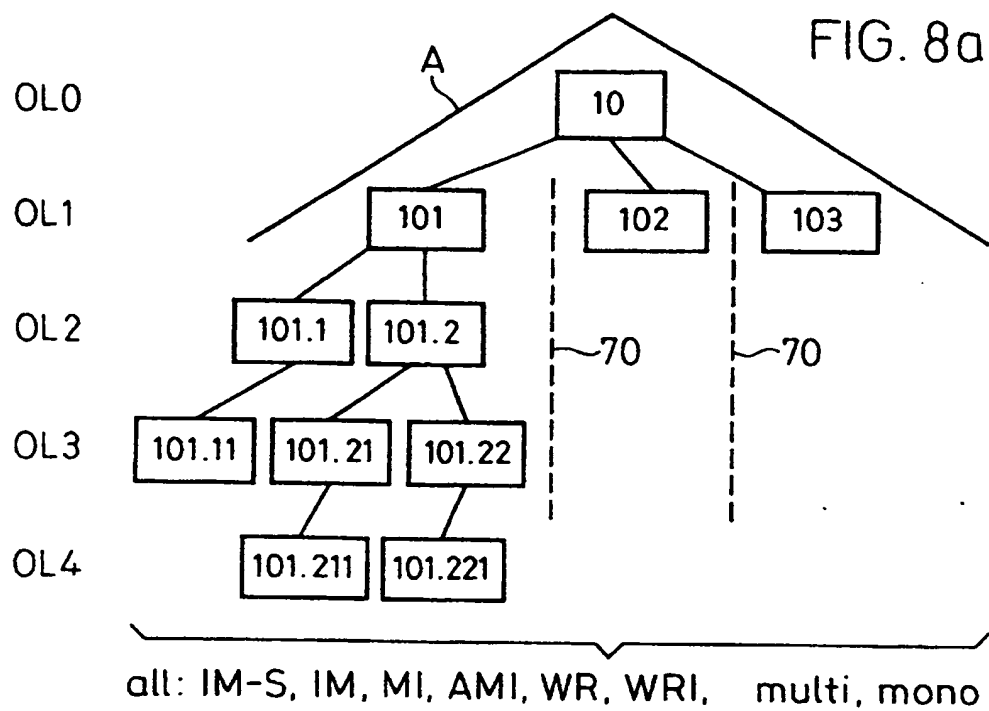


FIG. 6

6/11



7/11

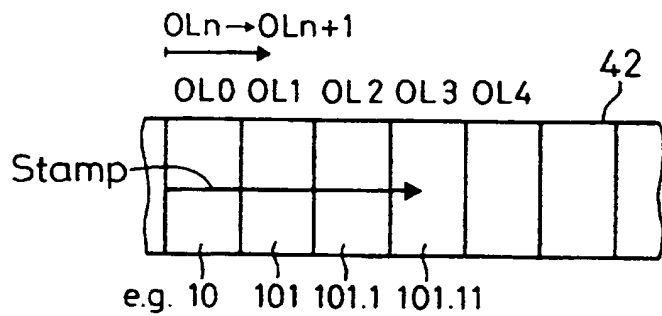


FIG. 9

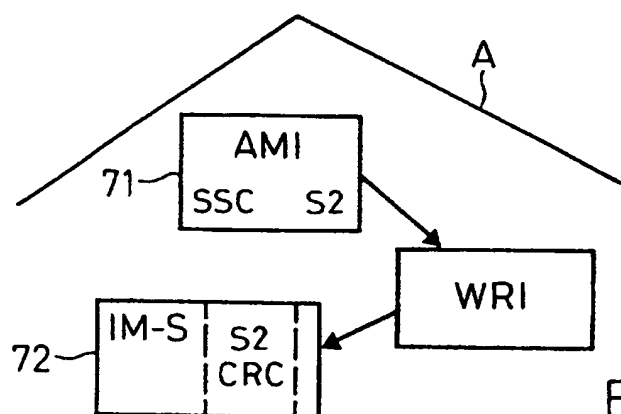
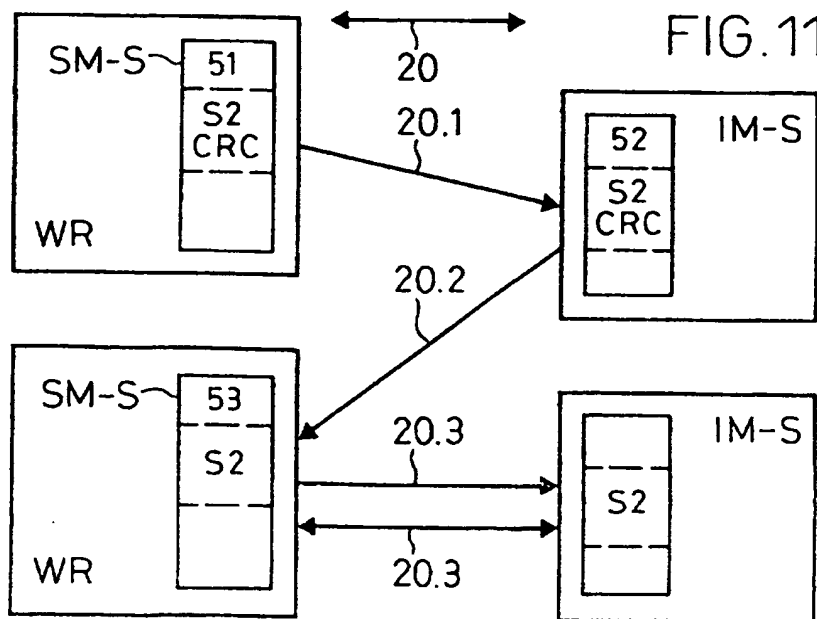
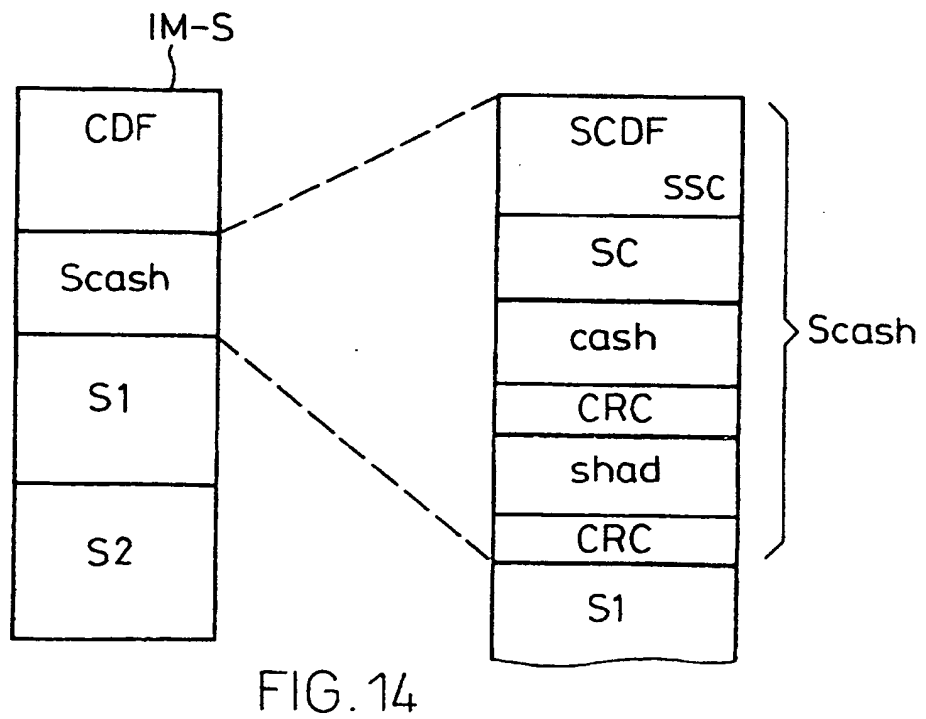
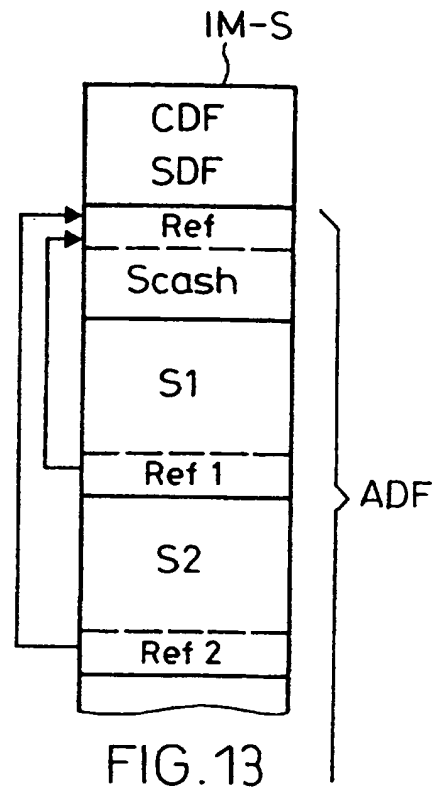
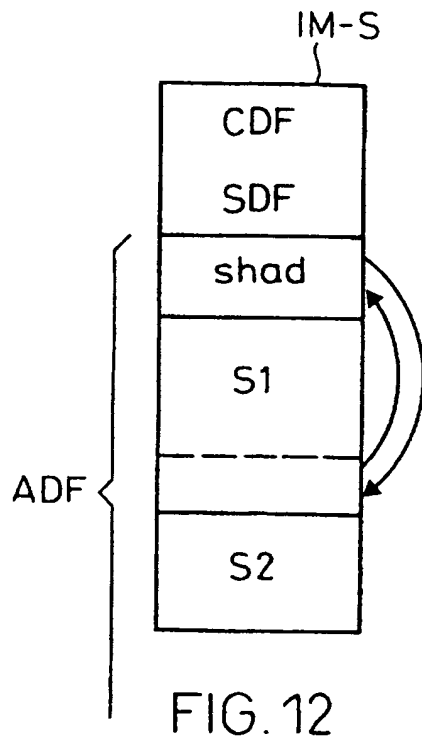


FIG. 10

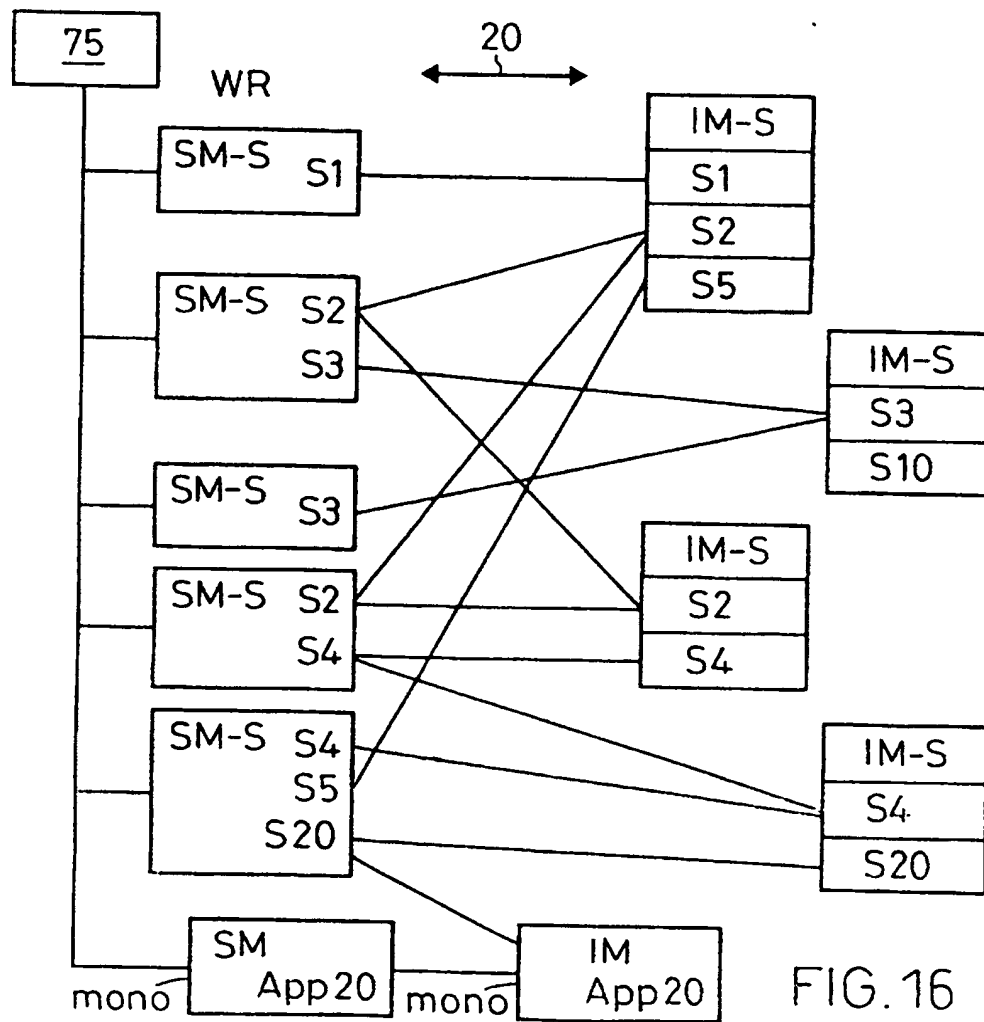
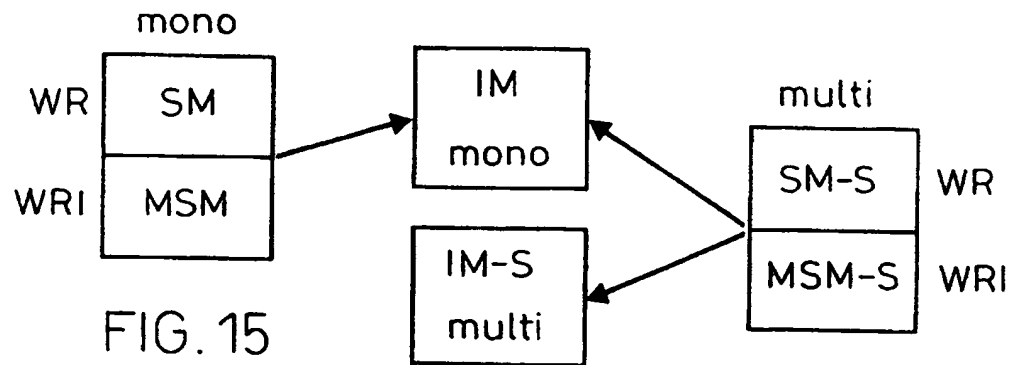


8/11





9/11



10/11

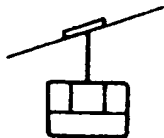
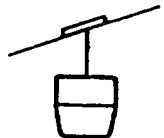




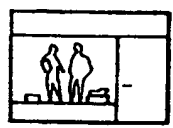
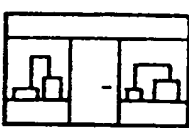



Scash (S1,S2,S3,S4) SSC1	S1, S2 S3, S4	
S1 SSC1	App1	
S2 SSC2	App2	
S3 SSC3	App3	   
S4 SSC4	App4	  
S5 SSC5	App5	 
cash S5		

FIG. 17

11/11

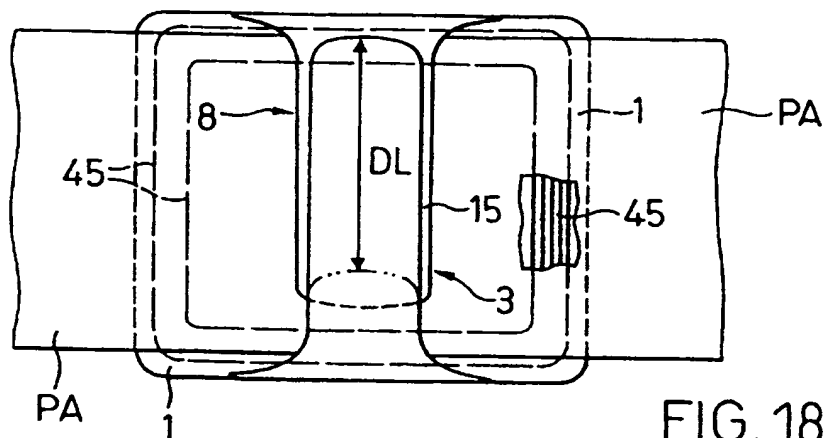


FIG. 18a

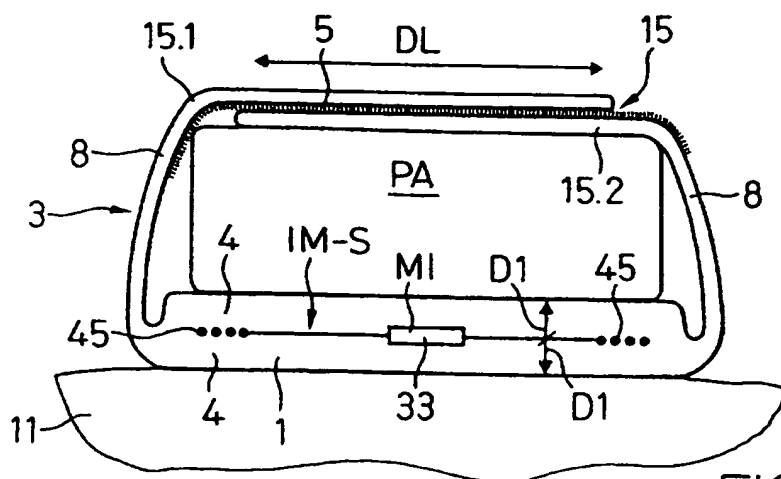


FIG. 18b

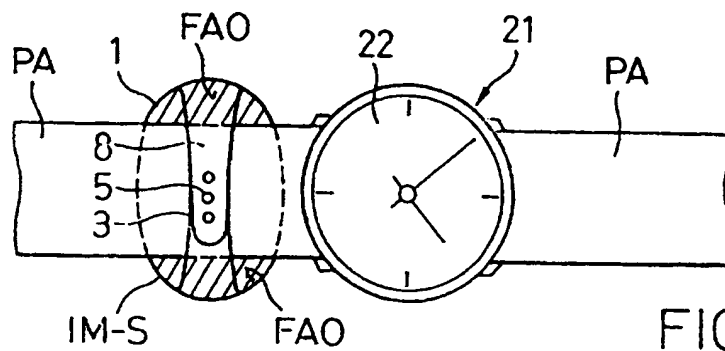


FIG. 19

# INTERNATIONAL SEARCH REPORT

International Application No.

PCT/CH 97/00063

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G07F/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 292 248 A (THE GENERAL ELECTRIC COMPANY, P.L.C.) 23 November 1988 see claims 1,3	1,2
A	DE 37 40 794 A (RODRIGUEZ, P. ET AL.) 15 June 1989 see claim 1	1,19,25, 26
A	FR 2 591 008 A (TOSHIBA K.K.) 5 June 1987 see claim 1	1,3-5
A	EP 0 617 387 A (TOSHIBA K.K.) 28 September 1994 see claims 1,6	1,3,5, 10,14, 15,17,23
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

13 May 1997

Date of mailing of the international search report

22.05.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Authorized officer

Herskovic, M

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/CH 97/00063

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 92 13322 A (GEMPLUS CARD INTERNATIONAL) 6 August 1992 see claims 1,4 ---	1,3-6,8, 16
A	EP 0 332 117 A (TOSHIBA K.K.) 13 September 1989 see claims 1,10 ---	1,3,4,6, 9,14,23
A	EP 0 644 513 A (AT & T CORP.) 22 March 1995 see claims 1,3,11 ---	1,3,5
A	FR 2 606 909 A (TOSHIBA K.K.) 20 May 1988 see claim 1 -----	1,7

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Application No  
PCT/CH 97/00063

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 292248 A	23-11-88	GB 2204973 A AU 1643488 A JP 1064033 A	23-11-88 24-11-88 09-03-89
DE 3740794 A	15-06-89	NONE	
FR 2591008 A	05-06-87	JP 62159295 A JP 62128388 A JP 62128390 A DE 3635409 A US 4887234 A	15-07-87 10-06-87 10-06-87 04-06-87 12-12-89
EP 617387 A	28-09-94	JP 6274397 A US 5517014 A	30-09-94 14-05-96
WO 9213322 A	06-08-92	FR 2673476 A DE 69205425 D DE 69205425 T EP 0589884 A ES 2082451 T JP 6504862 T US 5473690 A	04-09-92 16-11-95 21-03-96 06-04-94 16-03-96 02-06-94 05-12-95
EP 332117 A	13-09-89	JP 1229393 A JP 2050286 A DE 68915186 D DE 68915186 T US 5097118 A	13-09-89 20-02-90 16-06-94 25-08-94 17-03-92
EP 644513 A	22-03-95	US 5544246 A CA 2131510 A JP 7152837 A NO 943457 A	06-08-96 18-03-95 16-06-95 20-03-95
FR 2606909 A	20-05-88	JP 2537199 B JP 63000788 A DE 3720394 A DE 3733794 A FR 2600446 A US 4833595 A	25-09-96 05-01-88 23-12-87 17-03-88 24-12-87 23-05-89

### Information on patent family members

PCT/CH 97/00063

Form PCT/ISA/210 (patent family annex) (July 1992)

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/CH 97/00063

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
IPK 6 G07F/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 6 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 292 248 A (THE GENERAL ELECTRIC COMPANY, P.L.C.) 23. November 1988 siehe Ansprüche 1,3 ---	1,2
A	DE 37 40 794 A (RODRIGUEZ, P. ET AL.) 15. Juni 1989 siehe Anspruch 1 ---	1, 19, 25, 26
A	FR 2 591 008 A (TOSHIBA K.K.) 5. Juni 1987 siehe Anspruch 1 ---	1, 3-5
A	EP 0 617 387 A (TOSHIBA K.K.) 28. September 1994 siehe Ansprüche 1,6 ---	1, 3, 5, 10, 14, 15, 17, 23
-/--		

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

\*A\* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

\*E\* Älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

\*L\* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

\*O\* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

\*P\* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

\*T\* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

\*X\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

\*Y\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

\*A\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

13. Mai 1997

Abmeldedatum des internationalen Recherchenberichts

22.05.97

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Herskovic, M



# INTERNATIONALER RECHERCHENBERICHT

Ink. onales Aktenzeichen  
PCT/CH 97/00063

C(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 92 13322 A (GEMPLUS CARD INTERNATIONAL) 6.August 1992 siehe Ansprüche 1,4 ---	1,3-6,8, 16
A	EP 0 332 117 A (TOSHIBA K.K.) 13.September 1989 siehe Ansprüche 1,10 ---	1,3,4,6, 9,14,23
A	EP 0 644 513 A (AT & T CORP.) 22.März 1995 siehe Ansprüche 1,3,11 ---	1,3,5
A	FR 2 606 909 A (TOSHIBA K.K.) 20.Mai 1988 siehe Anspruch 1 -----	1,7

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/CH 97/00063

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 292248 A	23-11-88	GB 2204973 A AU 1643488 A JP 1064033 A	23-11-88 24-11-88 09-03-89
DE 3740794 A	15-06-89	KEINE	
FR 2591008 A	05-06-87	JP 62159295 A JP 62128388 A JP 62128390 A DE 3635409 A US 4887234 A	15-07-87 10-06-87 10-06-87 04-06-87 12-12-89
EP 617387 A	28-09-94	JP 6274397 A US 5517014 A	30-09-94 14-05-96
WO 9213322 A	06-08-92	FR 2673476 A DE 69205425 D DE 69205425 T EP 0589884 A ES 2082451 T JP 6504862 T US 5473690 A	04-09-92 16-11-95 21-03-96 06-04-94 16-03-96 02-06-94 05-12-95
EP 332117 A	13-09-89	JP 1229393 A JP 2050286 A DE 68915186 D DE 68915186 T US 5097118 A	13-09-89 20-02-90 16-06-94 25-08-94 17-03-92
EP 644513 A	22-03-95	US 5544246 A CA 2131510 A JP 7152837 A NO 943457 A	06-08-96 18-03-95 16-06-95 20-03-95
FR 2606909 A	20-05-88	JP 2537199 B JP 63000788 A DE 3720394 A DE 3733794 A FR 2600446 A US 4833595 A	25-09-96 05-01-88 23-12-87 17-03-88 24-12-87 23-05-89

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/CH 97/00063

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2606909 A		US 4901276 A	13-02-90
-----			